DoD CLASS 3 PKI Interoperability

LCDR Paul Friedrichs

PKI Chief Engineer

friedrip@ncr.disa.mil

15 June 2000

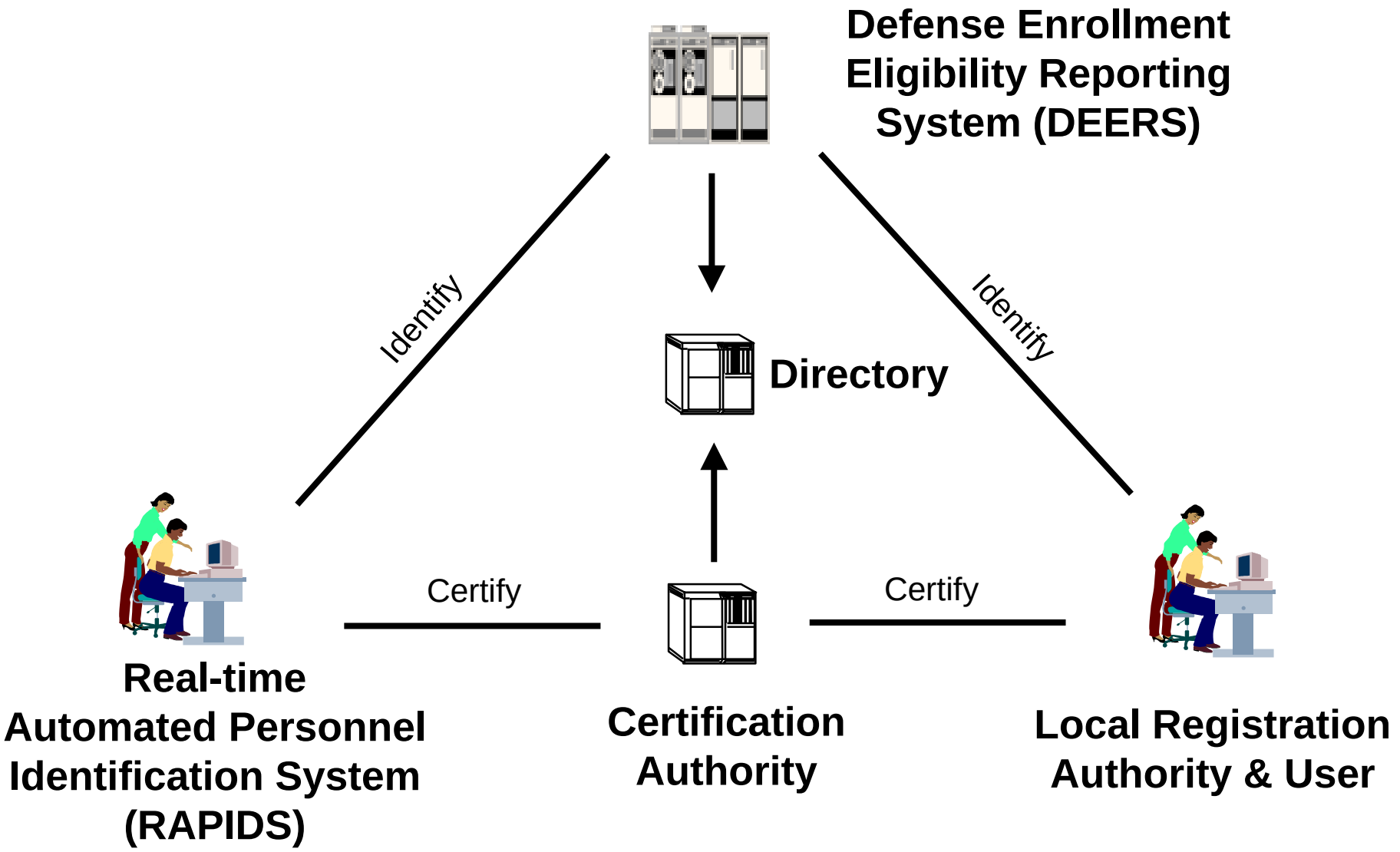
Current Characteristics (Release 1)

- Identity - not privilege or attributes
  - E-mail address in optional second cert
- Relatively static names - flat directory
- Few, centralized CAs - minimize O&M
- User keys in software - encourage use of PKI
- CRLs

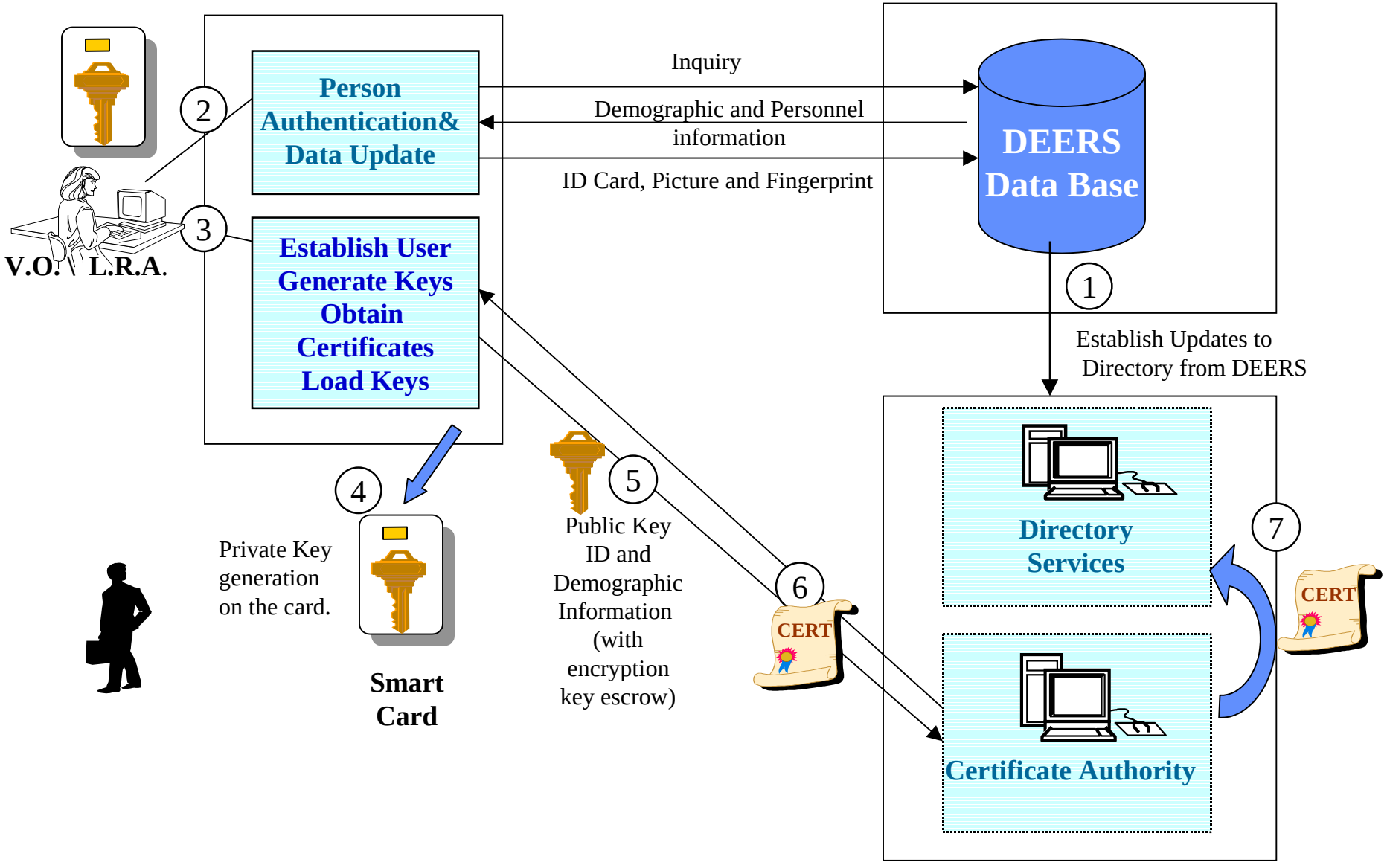
Release 2 (Imminent)

- Asserting Class 3 (FIPS level 3 CAs)
- Encryption key escrow & recovery
- Registration using CMC
- One ID cert - DS / NR
  - Optionally two additional e-mail certs
    - DS / NR
    - KE

Release 3 (Dec 00)



Release 3 Integrated Process



Release 3 (Dec 00)

- For those users in DEERS
  - Refer to DEERS to
    - Identify users
    - Obtain name of users
  - Use RAPIDS to register at least some users
    - Private keys on CAC
      - JavaCard, Open Platform
      - Possibly use certificatePolicies extension to distinguish
- Adding OCSP
- Release 1-3 total about $1-2 million “GOTS”

Strategy

- Client neutrality - key holder interoperability
- Participate in Fed Bridge CA - RP interop
- Multi-vendor infrastructure - limit risk
- Few registration protocols - limit O&M / risk
- View PKI, Smart Cards & Directories as related but separate challenges

- Relying Party interoperability without losing private key holder interoperability
- COTS without losing vendor-neutrality
- Outsource when / where possible

Current Interoperability with the PKI

- IETF PKIX & FedPKI profiles
- PKCS#12 (or CAPI and product that supports)
- Able to trust new roots and chain certs

- Name and certs exist prior to application
- LDAP
- userCertificate (not userSMIMECertificate)

- Interface Spec & App Enabling Guidelines
  - Need to also address infrastructure internals

Product Support

- Do not require e-mail address in certs
- Multi-valued userCertificate directory attribute
- Transparent key recovery
- Perhaps CN removed from DN

Multi-vendor Class 3 Infrastructure

- Desire more than one CA product in system
- No connection between key and CA vendor
  - Must not require same vendor software for use
- Require escrow and recovery
  - System likely to remain separate for each vendor
- CA / Directory interface currently LDAP over client-authenticated SSL
- Registration
  - RAPIDS / CAC currently CMC - should consider others
  - Software users using web-based shared secret
    - Possibly no longer worth emulating
- DEERS / CA population management interface
  - Revoke when leave population

Interoperability Challenges Where We Especially Need Your Help

- Use / meaning of nonRepudiation keyUsage ?
- DSS: RSA , SHA-1 & (X9.31 or PKCS#1 ?)
- Revocation mechanisms (& scalability)
- Standard registration protocol(s)
- Vendor-neutral cert management
- Standard timestamp / notary (& scalability ?)
- Do not require object signing extended key usage
- End user applications understand Bridge CA